



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/535,363	05/18/2005	Christian Kollmitzer	SONN:069US/10503277	7070
33425 7590 06/01/2009 FULBRIGHT & JAWORSKI L.L.P. 600 CONGRESS AVE. SUITE 2400 AUSTIN, TX 78701				
EXAMINER PYZOCHA, MICHAEL J				
ART UNIT		PAPER NUMBER		
2437				
MAIL DATE		DELIVERY MODE		
06/01/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/535,363

Applicant(s)

KOLLMITZER, CHRISTIAN

Examiner

MICHAEL PYZOSHA

Art Unit

2437

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 April 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 11-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 11-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SF/ICE)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 11-21 are pending.
2. Amendment filed 04/14/2009 has been received and considered.

Claim Rejections - 35 USC § 112

The rejection under the second paragraph of 35 U.S.C. 112 has been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 11-16 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Elliott et al. (US 6895091).

As per claim 11, Elliott et al. discloses a communication system using quantum cryptography comprising: subscriber stations connected to one or more quantum channels (see the Hosts in FIG. 5 and column 4 line 54 through column 5 line 27); one or more quantum-cryptographic device associated with the one or more quantum channels for generating a quantum key during use (see column 10 lines 45-63 and

column 11 lines 58-62); and several interconnected switching stations that, during use, communicate via public lines, using encryption agreed upon, without quantum-cryptographic key exchange; wherein, during use, the subscriber stations are connected to the switching stations via the one or more quantum channels that generate a respective temporary quantum key and are adapted to communicate via public lines using the quantum key (see column 10 line 64 through column 11 line 28).

As per claims 12-14 Elliott et al. discloses the switching stations have a source of photons and a photon detector and the subscriber stations comprise a photon detector (see column 8 lines 56-67 where each node must be able to create and detect photons to be able to communicate of a quantum channel).

As per claim 15, Elliott et al. discloses the switching stations are interconnected at least partially by point-to-point links (see FIG. 5 and column 4 line 54 through column 5 line 27 where router 525 can communicate with any other router).

As per claim 16, Elliott et al. discloses the switching stations are at least partially hierarchically interconnected (see FIG. 5 and column 4 line 54 through column 5 line 27 where router 525 must communicate with router 520 to communicate with router 505 when using only secure channels).

As per claim 21, Elliott et al. discloses wherein, during use, authentication data transmitted between the switching stations are checked by the switching stations prior to the establishment of a communication between subscriber stations (see column 8 line 49-67).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elliott et al. as applied to claim 11 above, in view of Elliot (US 7457416).

As per claims 17 and 18, Elliott et al. discloses generating key bits between subscriber stations and their associated switching stations after a request for communication has been transmitted (see column 8 line 49 through column 9 line 28), but fails to explicitly disclose generating a separate bit sequence and wherein, during use, a switching station associated with a called subscriber station generates a third key bit sequence from the key bit sequences generated via the quantum channels and transmits this third key bit sequence to the called subscriber station which, using the key bit sequence known to it and generated by it together with the associated switching station, from the third key bit sequence generates the key bit sequence generated on the part of the calling subscriber station, which then finally is used as a mutual key for the communication between the subscriber stations.

However, Elliott teaches such a quantum key agreement protocol (see FIG. 4 and column 6 line 48 through column 7 line 38).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the specific key agreement protocol of Elliott in the Elliott et al. system.

Motivation to do so would have been to allow for user devices to share a common secret key over an insecure network (see Elliott column 2 lines 41-44).

7. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Elliot et al. as applied to claim 11 above, in view of Menezes et al. (Handbook of Applied Cryptography).

As per claim 19, Elliot et al. fails to explicitly disclose discarding the quantum keys at the end of a communication.

However, Menezes et al. teaches discarding a key after a communication (see page 553).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to discard the quantum key of Elliot et al. after a communication.

Motivation to do so would have been to limit the exposure of the key (see Menezes et al. page 553).

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Elliott et al. as applied to claim 11 above, in view of Townsend et al. (US 5850441).

As per claim 20, Elliott et al. fails to explicitly disclose discarding the quantum keys at the end of communications of when eavesdropping is detected.

However, Townsend et al. teaches such discarding (see column 3 lines 29-48).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to discard the keys of the Elliott et al. system.

Motivation, as recognized by one of ordinary skill in the art, would have been to protect the security of the system.

Response to Arguments

9. Applicant's arguments filed 04/13/2009 have been fully considered but they are not persuasive. Applicant argues that Elliot '091 fails to disclose using encryption agreed upon, without quantum-cryptographic key exchange; Elliot '416 fails to teach the limitations of claims 17 and 18 and Townsend fails to teach discarding a quantum key at the end of a communication.

With respect to Applicant's argument (see pages 5-6) that Elliot '091 fails to disclose using encryption agreed upon, without quantum-cryptographic key exchange; Applicant contends (see bottom of page 5) that in column 11 lines 4-13 Elliot '091 performs a quantum key exchange; no where in this cited portion is there a description of any type of key exchange. Furthermore, Elliot '091 discloses multiple nodes communicating using conventional (non-quantum) encryption techniques to encrypt and decrypt exchanged data (see column 12 lines 19-29 and lines 45-57). Therefore, Elliot discloses using encryption agreed upon, without quantum-cryptographic key exchange.

With respect to Applicant's argument (see pages 6-7) that Elliot '416 fails to teach the limitations of claims 17 and 18 because Elliot '416 teaches away from these limitations; the KDC acts as the switching station of the claim language and when

communication is requested each user device sends its user key to the KDC (see FIG 4 numerals 410, 420 and 430) which corresponds to the limitations of claim 17. Next, the third bit sequence generated in the claim 18 is taught by the generation of the shared key of Elliot '416. Therefore, Elliot '416 teaches the limitations of claims 17 and 18. Additionally, the rejection above has been updated to reflect the teachings of Elliot '091 (column8 lines 49 through column 9 line 28) that were mistakenly left out of the previous action with respect to the rejection of claims 17 and 18, as noted by the Applicant.

Applicant's argument that Townsend fails to teach discarding a quantum key at the end of a communication is moot in view of the new grounds of rejection put forth above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Examiner, Art Unit 2437